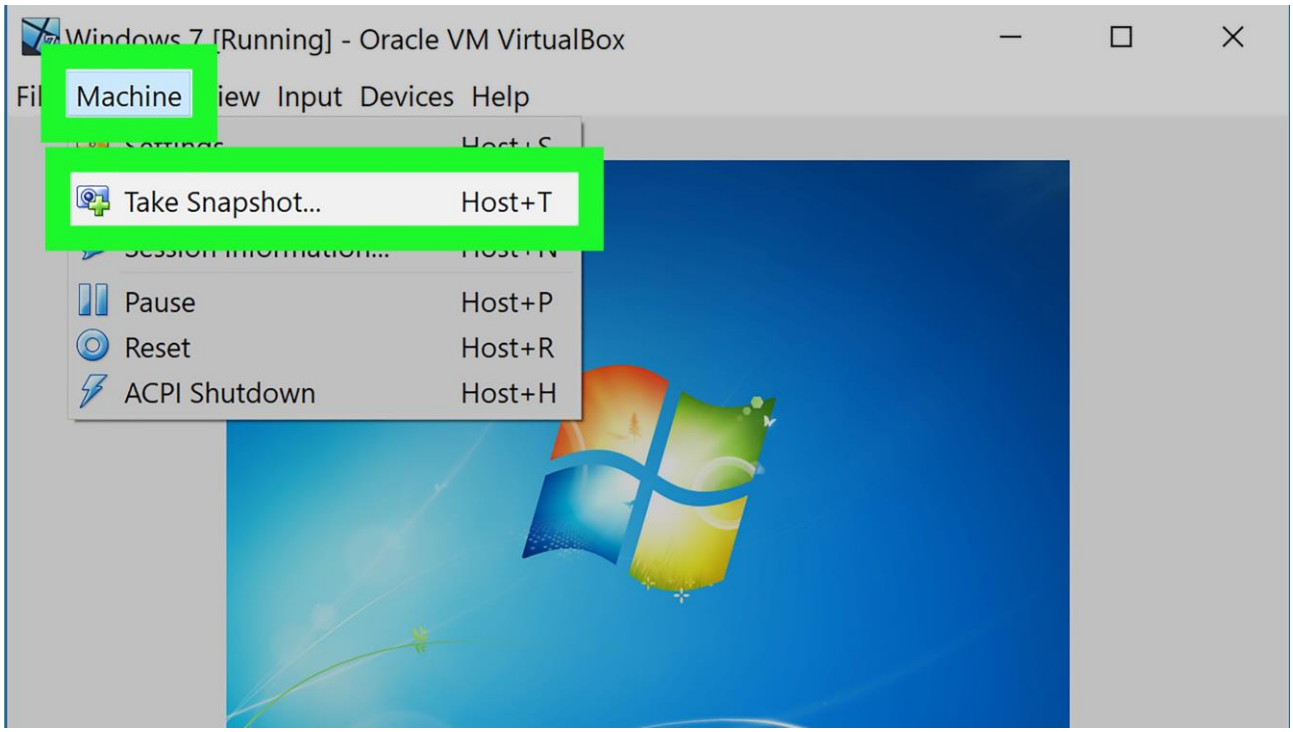
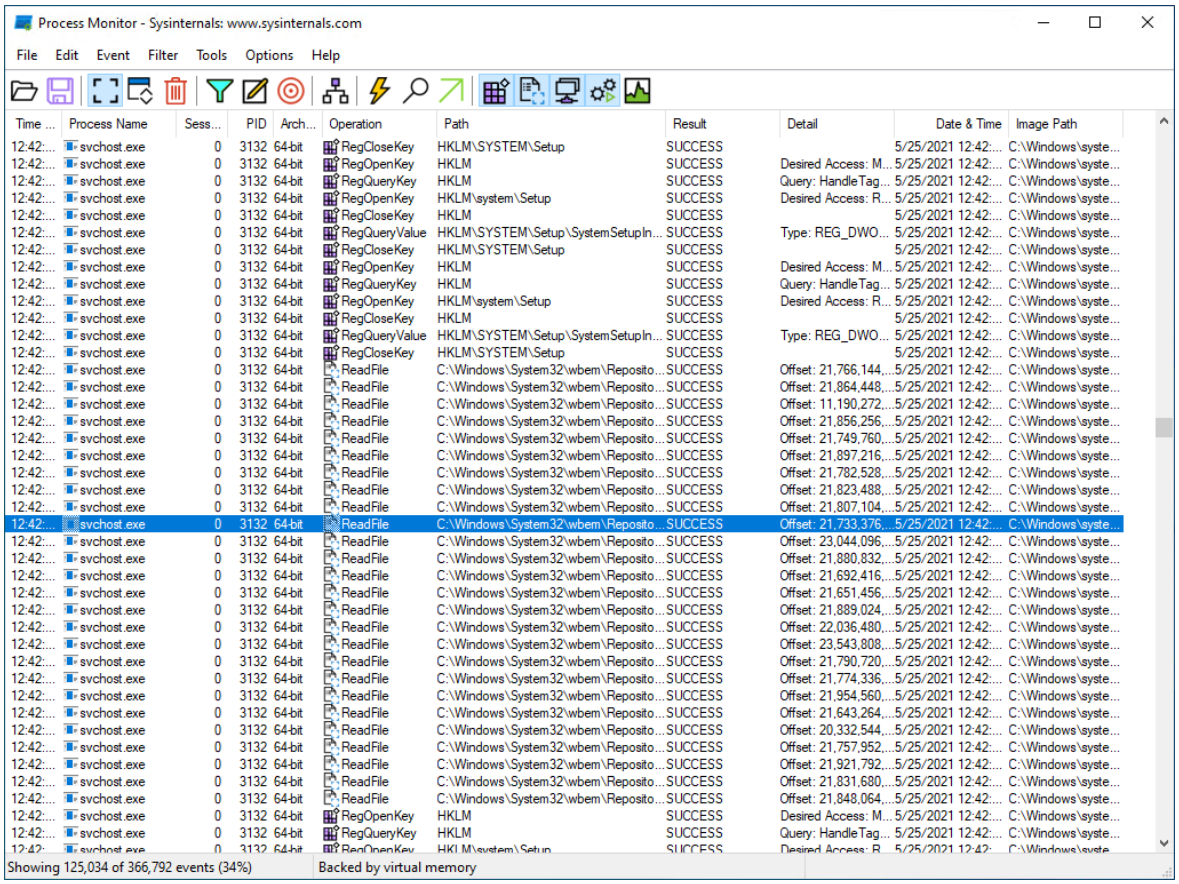
Per monitorare le attività di malware sul file system, in particolare le chiamate alla funzione `CreateFile` su path noti (come il path dell'eseguibile del malware), possiamo seguire questi passaggi:

1. **Creazione di un'istantanea della macchina VirtualBox:**
    - Aprire VirtualBox e selezionare la macchina Windows XP.
    - Fare clic su "Macchina" -> "Istantanea" -> "Prendi istantanea".
    - Dare un nome e una descrizione all'istantanea per ricordare lo stato della macchina in quel momento.



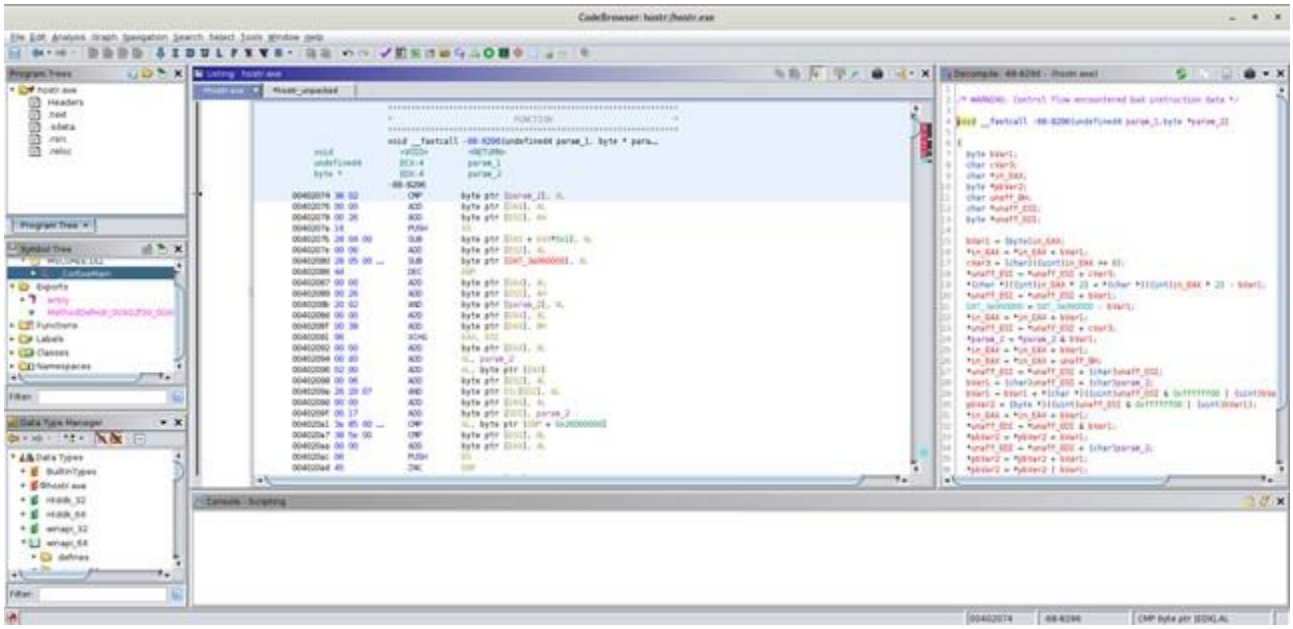
Monitoraggio delle chiamate alla funzione CreateFile:

- Scaricare e installare strumenti di monitoraggio come Process Monitor (Procmon) di Sysinternals.
- Configurare Process Monitor per monitorare le chiamate a `CreateFile`.
    - Aprire Process Monitor.
    - Applicare un filtro per le chiamate `CreateFile`:
        - Fare clic su "Filter" -> "Filter..." (o premere Ctrl+L).
        - Aggiungere una nuova regola: "Operation" -> "is" -> "CreateFile" -> "Include".
        - Aggiungere un'altra regola per il path dell'eseguibile del malware, se noto: "Path" -> "contains" -> "<path_to_malware>" -> "Include".
        - Fare clic su "Add" e poi su "OK" per applicare i filtri.



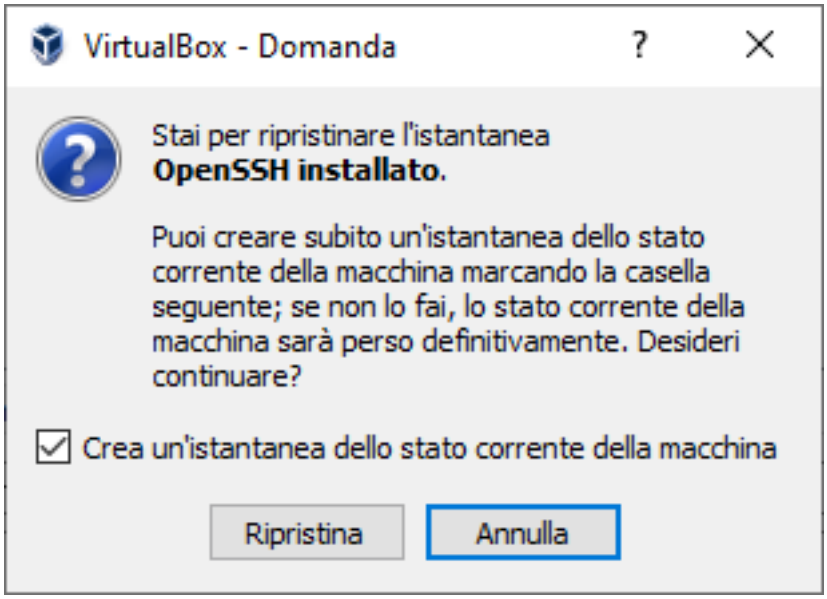
Analisi del malware:

- Eseguire il malware in un ambiente controllato.
- Osservare e registrare tutte le chiamate `CreateFile` nel path specificato.
- Analizzare i risultati per determinare le attività sospette o malevole.



Ripristino della macchina:

- Dopo aver completato l'analisi, è possibile ripristinare lo stato della macchina virtuale utilizzando l'istantanea creata precedentemente.
    - Selezionare la macchina virtuale in VirtualBox.
    - Fare clic su "Macchina" -> "Istantanea" -> selezionare l'istantanea e fare clic su "Ripristina".



Alternativa: Clonazione della macchina virtuale

1. **Clonare la macchina virtuale:**
    - Fare clic destro sulla macchina virtuale e selezionare "Clona"